UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/874,258	06/06/2001	Victor Larson	00479.00032	5950

22907 7590 08/09/2005

BANNER & WITCOFF
1001 G STREET N W
SUITE 1100
WASHINGTON, DC 20001

EXAMINER	
PHUNKULH, BOB A	
ART UNIT	**PAPER NUMBER**
2661	

DATE MAILED: 08/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/874,258	LARSON, VICTOR	
	Examiner	Art Unit	
	Bob A. Phunkulh	2661	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 May 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26,28-41,46-78 and 83* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25,27-33,36-38,41, 46-78 and 83* is/are rejected.

7)☒ Claim(s) *26,34,35,39 and 40* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/8/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This communication is in response to applicant's 05/24/2005 amendment(s)/response(s) in the application of **LARSON** for "**THIRD PARTY VPN CERTIFICATION**" filed 06/06/2001. The amendments/response to the claims have been entered. Claims 27, 42-45, 79-82, have been canceled. Claim 83 has been added. Claims 1-26, 28-41, 46-78, 83 are now pending.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 41 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 41, it is not clear what it meant by "receiving at the certification authority at least one VPN parameter for the VPN device that is not contained in the certificate request; and storing the at least one received VPN parameter that is not contained in the certificate request in an on-line database" as cited in the claim i.e. clarify the different between the "VPN parameter" in claim 24 and claim 41. Also, it is not clear where the VPN parameter is received from.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims *1-6, 8-25, 28, 33, 36-38, 46-53, 55-65, 67-78, 83* are rejected under 35 U.S.C. 102(b) as being anticipated by Muyiyappa et al. (US 6092200), hereinafter *Muyiyappa*.

Regarding claims 1 and 16, *Muniyappa* discloses a method and apparatus for establishing a virtual private network provides a technique for automatically configuring nodes of the network. Each node includes a public key and a private key for cryptographic communication in a first mode, such as RSA. Configuration data regarding communication in the network is provided to a master node. The configuration data is securely transferred into each other node from the master node. Nodes communicate with each other based upon a configuration data (see col. 2 lines 44-63).

Regarding claims 2 and 17, *Muniyappa* discloses the master node receiving requested public key or private key from the certification authority 80 (see col. 4 lines 43-56 and col. 5 lines 53-63).

Regarding claim 3, *Muniyappa* discloses sending the request from the first VPN device to the second VPN device sends the request to the secure domain name address associated with the second VPN device (received packets from the localized

computers include destination addresses (the secure domain name address associated with the VPN destination device), see col. 3 lines 63-67) .

Regarding claim 4, *Muniyappa* discloses the request from the first VPN device to the second VPN device for establishing the VPN further includes receiving a request for establishing the VPN from a client device that is associated with the first VPN device (each of the plurality of nodes are further connected to a LAN or localized computers, and connection are establish in response to a request received from the localized computers or LAN, see col. 3 lines 56-66).

Regarding claim 5, *Muniyappa* discloses the request received from the client device includes a destination designation for the VPN (received packets from the localized computers specifying addresses of source and destination nodes, see col. 3 lines 63-67).

Regarding claim 6, *Muniyappa* discloses the request received from the client device includes a source/destination designation for the VPN (received packets from the localized computers specifying addresses of source and destination nodes, see col. 3 lines 63-67).

Regarding claim 8, *Muniyappa* discloses the step of verifying at the first VPN device the second signed certificate having at least one verified VPN parameter for the

second VPN device (see col. 5 lines 48-63).

Regarding claim 9, *Muniyappa* discloses the step of verifying the second signed certificate includes a step of sending a request from the first VPN device to an on-line database (certification authority 80) for obtaining a public key associated with the second VPN device (see col. 5 lines 48-63).

Regarding claim 10, *Muniyappa* discloses the step of verifying at the second VPN device the first signed certificate having at least one verified VPN parameter for the first VPN device (col. 5 lines 42-46).

Regarding claim 11, *Muniyappa* disclose the step of verifying the first signed certificate includes a step of sending a request to an on-line database from the second VPN device for obtaining a public key associated with the first VPN device (sending request to certification authority 80, see col. 5 lines 48-63).

Regarding claim 12, *Muniyappa* discloses determining at the second VPN device whether a policy rule prevents a VPN connection to the first VPN device; and sending the reply to the first VPN device from the second VPN device when no policy rule prevents a VPN connection to the first VPN device, and not sending the reply to the first VPN when a policy rule prevents a VPN connection to the first VPN device (a "configuration," as used herein, refers to the ability of nodes to communicate with each

other over the established logical links using the virtual private network of this invention. Notably, only certain links are allowed; each allowed link being depicted in FIG. 1 according to Sender-Receiver notation, see col. 4 lines 24-33).

Regarding claims 13, 21, *Muniyappa* discloses the telecommunications network is the Internet (Internet/Intranet 40, see figure 1).

Regarding claims 14, 22, *Muniyappa* discloses establishing the VPN between the first and second VPN devices establishes a standing VPN connection (col. 2 lines 44-54; step 110 in figure 3).

Regarding claims 15, 23, *Muniyappa* discloses establishing the VPN between the first and second VPN devices establishes a VPN of opportunity (col. 2 lines 44-54; step 110 in figure 3).

Regarding claim 18, *Muniyappa* discloses the step of verifying at the second VPN device the first signed certificate having at least one verified VPN parameter for the first VPN device (see col. 5 lines 43-46).

Regarding claim 19, *Muniyappa* disclose the step of verifying the first signed certificate includes a step of sending a request to an on-line database from the second VPN device for obtaining a public key associated with the first VPN device (sending

request to certification authority 80, see col. 5 lines 48-63).

Regarding claim 20, *Muniyappa* discloses determining at the second VPN device whether a policy rule prevents a VPN connection to the first VPN device; and sending the reply to the first VPN device from the second VPN device when no policy rule prevents a VPN connection to the first VPN device, and not sending the reply to the first VPN when a policy rule prevents a VPN connection to the first VPN device (a "configuration," as used herein, refers to the ability of nodes to communicate with each other over the established logical links using the virtual private network of this invention. Notably, only certain links are allowed; each allowed link being depicted in FIG. 1 according to Sender-Receiver notation, see col. 4 lines 24-33).

Regarding claim 24, *Muniyappa* discloses a method for creating a virtual private network (VPN) over a telecommunications network, comprising steps of:

sending a certificate request for a virtual private network (VPN) device to a certification authority connected to the telecommunications network, the certificate request including at least one VPN parameter that will be used by the VPN device for establishing a VPN over the telecommunications network (each nodes requests signed certificate to a certification authority 80, see col. 4 lines 42-56);

receiving a signed certification from the certification authority, the signed certification containing the at least one VPN parameter contained in the certificate

request (the CA 80 assigned the certifications i.e. public and private keys for setting up VPN, see col. 4 lines 42-56);

configuring the VPN device to operate in accordance with the at least one VPN parameter contained in the signed certificate (see col. 4 line 64 to col. 5 line 12),

exchanging the signed certificate with another VPN device at a selected telecommunications network address; and

establishing the VPN in accordance with the least one VPN parameter contained in the signed certificate (establishing the VPN links among each of the nodes, see claim 1).

Regarding claim 25, *Muniyappa* discloses the certificate request includes at least one telecommunications network address (master node address information) that the VPN device will use for establishing a VPN device (see col. 5 lines 51-63).

Regarding claim 28, *Muniyappa* the step of establishing the VPN is further based on a source and destination name pair (VPN connection is establish based on the received packets source addresses and destination address at each nodes, see col. 3 lines 63-67).

Regarding claim 30, *Muniyappa* discloses the step of establishing the VPN is further based on at least one rule allowing a VPN connection to the selected telecommunications network address (master node address information, see col. 5 lines 51-63).

Regarding claim 33, *Muniyappa* discloses the telecommunications network is the Internet.(Internet/Intranet 40, see figure 1).

Regarding claim 36, *Muniyappa* disclose sending at least one VPN parameter for the VPN device that is not contained in the certificate request to the certification authority for verification by the certificate authority (see col. 5 lines 43-47).

Regarding claim 37, *Muniyappa* discloses receiving the certificate request for the VPN device from the VPN device at the certification authority; verifying at the certification authority the at least one VPN parameter contained in the certificate request; and sending the signed certification to the VPN device when each VPN parameter contained in the certificate request is verified (see col. 5 lines 47-57).

Regarding claim 38, *Muniyappa** the certificate request includes at least one telecommunications network address that the VPN device will use as a client network address for a VPN established through the VPN device, wherein the step of verifying verifies each telecommunication network address contained in the certificate request (providing the certification authority 80 with master's address for verification, see col. 5 lines 47-57) .

Regarding claim 46, *Muniyappa* discloses a virtual private network (VPN) device, comprising:

a memory containing a certificate that has been signed by a certification authority, the signed certificate containing at least one VPN parameter for the VPN device that has been verified by the certification authority (each node stores a public key and a private key for secure communication in a first cryptographic mode, such as public key cryptography, see col. 2 lines 55-63); and

a processor programmed to receive a request for establishing a VPN between the VPN device and a second VPN device and respond to the request by sending the signed certificate over a telecommunications network to the second VPN device based on the received request (nodes communicate with each other based upon a configuration data, where the configuration data includes cryptographic key, see abstract).

Regarding claim 47, *Muniyappa* discloses the request is received from the second VPN device, and a signed certificate for the second VPN device, the signed certificate for the second VPN device containing at least one VPN parameter for the second VPN device that has been verified by a certification authority (nodes uses the secret key i.e. signed certificates to communicates among each other, see col. 3 lines 10-15).

Regarding claim 48, *Muniyappa* discloses the processor verifies the signed certificate for the second VPN device before sending the signed certificate to the second VPN device (each nodes have pre-assigned keys or signed certificates, col. 2 lines 55-63).

Regarding claim 49, *Muniyappa* discloses the processor verifies the signed certificate for the second VPN device using a public key associated with the second VPN device (see col. 5 lines 47-57).

Regarding claim 50, *Muniyappa* discloses the processor establishes a VPN based on each verified VPN parameter for the VPN device and based each verified VPN parameter for the second VPN device (see col. 5 lines 47-57).

Regarding claim 51, *Muniyappa* discloses the request from the first VPN device to the second VPN device for establishing the VPN further includes receiving a request for establishing the VPN from a client device that is associated with the first VPN device (each of the plurality of nodes are further connected to a LAN or localized computers, and connection are establish in response to a request received from the localized computers or LAN, see col. 3 lines 56-66).

Regarding claim 52, *Muniyappa* discloses the request received from the client device includes a destination designation for the VPN (received packets from the

localized computers specifying addresses of source and destination nodes, see col. 3 lines 63-67).

Regarding claim 53, *Muniyappa* discloses the request received from the client device includes a source/destination designation for the VPN (received packets from the localized computers specifying addresses of source and destination nodes, see col. 3 lines 63-67).

Regarding claim 55, *Muniyappa* discloses determining at the second VPN device whether a policy rule prevents a VPN connection to the first VPN device; and sending the reply to the first VPN device from the second VPN device when no policy rule prevents a VPN connection to the first VPN device, and not sending the reply to the first VPN when a policy rule prevents a VPN connection to the first VPN device (a "configuration," as used herein, refers to the ability of nodes to communicate with each other over the established logical links using the virtual private network of this invention. Notably, only certain links are allowed; each allowed link being depicted in FIG. 1 according to Sender-Receiver notation, see col. 4 lines 24-33).

Regarding claim 56, *Muniyappa* discloses the telecommunications network is the Internet (internet/intranet 40, see figure1).

Regarding claim 57, *Muniyappa* discloses establishing the VPN between the first and second VPN devices establishes a standing VPN connection (col. 2 lines 44-54; step 110 in figure 3).

Regarding claim 58, *Muniyappa* discloses establishing the VPN between the first and second VPN devices establishes a VPN of opportunity (col. 2 lines 44-54; step 110 in figure 3).

Regarding claim 59, *Muniyappa* discloses the VPN device is one of a VPN concentrator, a router, a firewall and a host computer (the plurality nodes 20, 22, 24, 36, see col. 3 lines 56-67).

Regarding claim 60, *Muniyappa* discloses a computer-readable medium containing computer executable instructions for performing steps of:

sending a request from a first VPN device to a second VPN device for establishing a VPN between the first and second VPN devices, the request including a first signed certificate having at least one verified VPN parameter for the first VPN device (the plurality of nodes establish VPN links using based on the configuration information i.e. signed public key, private key, and secret key cryptography techniques, see claim 1) ; and

receiving a reply at the first VPN device from the second VPN device, the reply including a second signed certificate having at least one verified VPN parameter for the second VPN device (see col. 5 lines 37-46); and

establishing the VPN between the first and second VPN devices based each verified VPN parameter for each of the first and second VPN devices the plurality of nodes establish VPN links using based on the configuration information i.e. signed public key and private key, see claim 1).

Regarding claim 61, *Muniyappa* discloses sending a request from the first VPN device to an on-line database connected to the telecommunications network for a secure domain name address associated with the second VPN device (see col. 5 lines 43-47).

Regarding claim 62, *Muniyappa* discloses sending the request from the first VPN device to the second VPN device sends the request to the secure domain name address associated with the second VPN device (see col. 5 lines 43-47).

Regarding claim 63, *Muniyappa* discloses the request from the first VPN device to the second VPN device for establishing the VPN further includes receiving a request for establishing the VPN from a client device that is associated with the first VPN device (each of the plurality of nodes are further connected to a LAN or localized computers, and connection are establish in response to a request received from the localized

computers or LAN, see col. 3 lines 56-66).

Regarding claim 64, *Muniyappa* discloses the request received from the client device includes a destination designation for the VPN (received packets from the localized computers specifying addresses of source and destination nodes, see col. 3 lines 63-67).

Regarding claim 65, *Muniyappa* discloses the request received from the client device includes a source/destination designation for the VPN (received packets from the localized computers specifying addresses of source and destination nodes, see col. 3 lines 63-67).

Regarding claim 67, *Muniyappa* discloses the step of verifying at the first VPN device the second signed certificate having at least one verified VPN parameter for the second VPN device (see col. 5 lines 40-46).

Regarding claim 68, *Muniyappa* discloses verifying the second signed certificate includes a step of sending a request from the first VPN device to an on-line database for a public key associated with the second VPN device (see col. 5 lines 48-57).

Regarding claim 69, *Muniyappa* discloses verifying at the second VPN device the first signed certificate having at least one verified VPN parameter for the first VPN

device (see col. 5 lines 48-57).

Regarding claim 70, *Muniyappa* discloses the step of verifying the first signed certificate includes a step of sending a request to an on-line database from the second VPN device for a public key associated with the first VPN device (see col. 5 lines 48-57).

Regarding claim 71, *Muniyappa* discloses determining at the second VPN device whether a policy rule prevents a VPN connection to the first VPN device; and sending the reply to the first VPN device from the second VPN device when no policy rule prevents a VPN connection to the first VPN device, and not sending the reply to the first VPN when a policy rule prevents a VPN connection to the first VPN device (a "configuration," as used herein, refers to the ability of nodes to communicate with each other over the established logical links using the virtual private network of this invention. Notably, only certain links are allowed; each allowed link being depicted in FIG. 1 according to Sender-Receiver notation, see col. 4 lines 24-33).

Regarding claim 72, *Muniyappa* discloses the telecommunications network is the Internet (Internet/Intranet 40, see figure 1).

Regarding claim 73, *Muniyappa* discloses establishing the VPN between the first and second VPN devices establishes a standing VPN connection (col. 2 lines 44-54; step 110 in figure 3).

Regarding claim 74, *Muniyappa* discloses establishing the VPN between the first and second VPN devices establishes a VPN of opportunity (col. 2 lines 44-54; step 110 in figure 3).

Regarding claim 75, *Muniyappa* discloses a computer-readable medium containing computer-executable instructions for performing steps of:

sending a certificate request for a virtual private network device to a certification authority connected to the telecommunications network, the certificate request including at least one VPN parameter that will be used by the VPN device for establishing a VPN over the telecommunications network (each node queries the certification authority to receive the public key by providing the certification authority with the master's address information so that the certification authority can look-up the appropriate public key (VPN parameter) for the master based upon its address information, see col. 5 lines 52-57);

receiving a signed certification from the certification authority, the signed certification containing the at least one VPN parameter contained in the certificate request (see col. 5 lines 58-60); and

configuring the VPN device to operate in accordance with the at least one VPN parameter contained in the signed certificate (col. 9 lines 59-62).

Regarding claim 76, *Muniyappa* disclose the certificate request includes at least one telecommunications network address that the VPN device will use as a client network address for a VPN established through the VPN device (master's network address, see col. 5 lines 53-57).

Regarding claim 77, *Muniyappa* discloses the certificate request includes a range of telecommunications network addresses (the master node address information) that the VPN device will use for VPNs established through the VPN device, and wherein the step of verifying verifies the range of telecommunications network addresses contained in the certificate request (see col. 5 lines 51-63).

Regarding claim 78, *Muniyappa* discloses the telecommunications network is the Internet (Internet/Intranet 40, see figure 1).

Regarding claim 83, *Muniyappa* disclose the second certification authority and the certification authority are that same (Certification Authority 80, see figure 1).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 7, 29, 54, 66 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Muniyappa*.

Regarding claims 7, 29, 54, and 66, *Muniyappa* fails to disclose the destination designation includes a wild card designation. However, it would have been obvious to one having ordinary skill in the art at the time of invention was made to designate the wild card destination just incase the designated receiver or destination is unable to receive the data at present time and forwarding the received data to it intended destination when available to receive the data –thus minimizing the network resources by releasing the connection once the data has been deliver to the wild card destination or the intended destination.

Claims 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Muniyappa* in view of *Genty* et al. (US 6,675,225), hereinafter *Genty*.

Regarding claim 31-32, fails to disclose establishing the VPN based on QOS or bandwidth limitation parameter.

Genty, on the other hand, discloses establishing the VPN based on QOS or bandwidth limitation parameter (see col. 6 lines 30-32).

Therefore, it would have been obvious to one having ordinary skill in the art at

the time of invention was made includes the teaching of *Genty* in the system taught by *Muniyappa* in order to efficiently use the limited network resources while providing user's demands.

Allowable Subject Matter

Claims 26, 34-35, 39, 40, objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any response to this action should be mailed to:

The following address mail to be delivered by the United States Postal Service (USPS) only:

Mail Stop _____
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

or faxed to:

(703) 872-9306, (for formal communications intended for entry)

Or:

The following address mail to be delivered by other delivery services (Federal Express (Fed Ex), UPS, DHL, Laser, Action, Purolater, Hand Delivery, etc.) as follow:

U.S. Patent and Trademark Office
220 20th Street South
Customer Window, Mail Stop _____

Crystal Plaza Two, Lobby, Room 1B03
Arlington, VA 22202.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to **Bob A. Phunkulh** whose telephone number is **(571) 272-3083.** The examiner can normally be reached on Monday-Tursday from 8:00 A.M. to 5:00 P.M. (first week of the bi-week) and Monday-Friday (for second week of the bi-week).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor **Chau Nguyen**, can be reach on **(571) 272-3126.** The fax phone number for this group is **(571) 273-8300.**

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Bob A. Phunkulh
Primary Examiner
TC 2600
Art Unit 2661
August 5, 2005

BOB PHUNKULH
PRIMARY EXAMINER